How cloud-based cyber security helped KPMG stay safe and connected

KPMG is a global organization of independent member firms based in 146 countries and territories, and employing nearly 227,000 people; from a few hundred staff members in smaller countries to tens of thousands in the larger firms. They all rely on KPMG's Information Technology Services (ITS) Global unit for key technology services.

Between 2015 and 2018, ITS Global assisted KPMG firms in moving to the Microsoft Office 365 cloud-based software suite and replacing on-premise data centers using Microsoft's Azure cloud hosting service. In 2019, KPMG and Microsoft strengthened their global relationship through a five-year agreement to expand KPMG's range of digital offerings with innovations in cloud-based audit capabilities, tax solutions and risk management.

The move to the cloud provided several advantages. Most notably, updates and new features can be pushed out across the global organization centrally rather than in each data center which can significantly reduce the time to deploy.

Brian Geffert, KPMG's Global Chief Information Security Officer, says the move to the cloud has made his job easier: "A consistent, centrally-controlled environment is easier to monitor than various data centers, making it possible to respond more quickly to security challenges. This has improved our security posture."

Securing KPMG's cloud

Geffert wanted to go further in securing KPMG's cloud. He did so by taking the same approach that KPMG firms have taken in other areas of their technology infrastructure: moving security software to the cloud and using Microsoft cloud-based security products.

This approach works well with the other Microsoft products and services used at KPMG. Although member firms may use other cloud-hosted services, Microsoft is the main provider which allowed Geffert to focus on developing 'Azure Global Cloud Security Guardrails', a set of rules for securing cloud instances that allow KPMG to maintain and support a common baseline across cloud platforms.

The project to expand cloud-based security took place during 2020, with several key goals. One was to implement Microsoft's cloud-based Security Information and Event Management (SIEM) product, Azure Sentinel. This is designed to integrate well with Microsoft Office 365 and can connect to other suppliers' security products. It also gives KPMG access to threat intelligence from Microsoft that draws on its monitoring of hundreds of millions of pieces of hardware: "It does the background work for us while we do the additional research," says Geffert.

Azure Sentinel took six months to implement in most KPMG firms. According to Geffert, it is much easier to update and maintain than the legacy systems it replaced, which took some months to upgrade from one version to the next:

"We can easily turn on security features and roll them out," he says of Azure Sentinel. "It upgrades more frequently, all in the background. It's night and day," he says.

The project also involved implementing Microsoft's Endpoint Detection and Response (Microsoft Defender for Endpoint) and Identity and Access Management (Microsoft Azure Active Directory) solutions on 260,000 laptops and over 300 identity repositories worldwide. The Defender for Endpoint work was completed in December 2020, with Azure Active Directory following in February 2021. "If this were an add-on rather than integrated into the endpoint, we would be at a disadvantage," says Geffert.

Like many organizations, KPMG had to move rapidly to allow staff to work remotely during the COVID-19 pandemic and implemented the collaboration tool Microsoft Teams worldwide in less than three weeks to some 250,000 users globally: "That was the power of the cloud," Geffert says. This led to a further component being added to 2020's cloud-based security project: the introduction of Microsoft Cloud Application Security for Teams. Doing so was vital given how quickly KPMG firms adopted Microsoft Teams, which has changed the way many meetings and conferences take place.

Based in Bulgaria, the Netherlands, the United Kingdom, the United States and India, Geffert's own team had to implement this set of projects while working remotely. "We've never done this before," he says, adding that it was a heavy lift. "Being able to do this while going through COVID-19 was unbelievable. Our teams were absolutely able to deliver."

Using in-house experience to help clients

KPMG's recent experience of implementing cloud-based security systems across the global organization means it is well-suited to help other complex organizations undertake similar projects of this scale. "KPMG professionals have a lot of experience using the tools," says Geffert.

Before deploying Microsoft software updates, we make sure to tailor the configurations and settings to meet our requirements. "Microsoft does a good job of anticipating the needs of its key customers and we configure those options in a manner that is appropriate for our industry and profession," says Geffert. This can mean postponing the introduction of new features until compatibility within the KPMG environment has been verified.

Since KPMG firms operate independently, we don't always want the data to flow freely within our organization, we may choose or be obliged not to share data with other KPMG entities. Geffert's team has made the adjustments accordingly — a capability other network-style multinational organizations with complex regulatory needs can draw on.

KPMG can also share the experience of automating much of the routine work previously carried out by their cybersecurity staff, which has allowed them to focus on more complex analysis. According to Geffert, this makes KPMG's Security Operations Center a more interesting and attractive place for cybersecurity specialists to work, which is vital to attracting and retaining tech talent.

Such automation can also help KPMG firms and their clients address emerging threats more effectively. Dealing with most warnings automatically creates time for expert staff to analyze and interpret patterns in low-level warnings — as they could play a key part in stopping the next such attack.

Overall, the move to cloud-based security shows how KPMG can solve a complex integration and transformation problem at a global scale, as it has achieved this for KPMG firms around the world. "When you look across the KPMG environment, we have different needs in our client base," says Geffert. "If other complex organizations are thinking about doing this, we can definitely help — sharing what we did on the journey and providing some valuable lessons."

home.kpmg/socialmedia

Designed by Evalueserve. | Publication name: How cloud-based cyber security helped KPMG stay safe and connected

Publication number: 137748-G | Publication date: October 2021